UPMC | University of Pittsburgh Medical Center

Innovative Medical & Information Technologies Center

Quantum One, Suite 079.1
200 Lothrop Street
Pittsburgh, PA 15213
1-877-37IMITS
Fax 412-432-7568
imits@upmc.edu

July 24, 2006

Department of Health and Human Services
200 Independence Avenue, SW
Room 434E
Washington, DC 20201

RE: IMDA RFI Response

Dear Sir or Madam:

I have enclosed, for your review, comments from the University of Pittsburgh Medical Center (UPMC) relating to the US Department of Health and Human Services *Request for Information: Voluntary Storage of Personal Data in Preparation for Emergencies* (71 FR 29642). UPMC is the premier health system in western Pennsylvania and one of the most renowned academic medical centers in the United States. As the area's only academic medical center, UPMC is a hub for specialized services and innovative research programs and technology. UPMC utilizes cutting-edge technologies developed in-house and in partnership with commercial entities to bridge the long distances between hospitals.

Recent events, such as Hurricane Katrina, have shown the spotlight on the challenges associated with providing emergency care during a crisis situation. These events have also indicated an increasing need to provide interoperability between healthcare providers as well as between healthcare payers and providers on a patient-by-patient basis. Each patient has their own unique clinical and financial healthcare needs. Often, multiple healthcare providers are rendering these services with no interoperability. The management of patients both from a clinical and financial perspective is daunting with duplication of services and data collection.

As such, UPMC appreciates the opportunity to comment on the voluntary storage of personal data in preparation for emergencies.

Sincerely,

Scott Gilstrap
Vice President, IMITs Center

Enclosure

CC George Huber
Loren Roth

UPMC | University of Pittsburgh Medical Center

US Department of Health & Human Services

Request for Information: Voluntary Storage of Personal Data in Preparation for Emergencies

Aspects of Emergency Preparedness, Response, and Recovery

Healthcare Passport
Secure Information Sharing and Authentication & Credentialing Card (SISAC)

This response to the US Department of Health and Human Services Request for Information: Voluntary Storage of Personal Data in Preparation for Emergencies documents the University of Pittsburgh Medical Center (UPMC)'s recommendations related to the availability and feasibility of private sector services through which individuals could voluntarily submit their personal information for storage so that they, their family members, or other designated individuals could access the information in an emergency.

Please contact Charles Boivin, Coordinator, Disaster Management Research, UPMC Innovative Medical and Information Technologies Center, at 412-432-7215 for questions related to this document.

Table of Contents

Background

In April 2004, President Bush called for the majority of Americans to have interoperable health records within 10 years. President Bush took action by signing an Executive Order establishing the position of the National Coordinator for Health Information Technology. Between 2004 and 2005, two of the leading companies who specialize in electronic health records (Eclipsys and Cerner) have seen an 18% to 27% increase in physicians' use of computers in healthcare settings, specifically in entering patient orders (Klas, 2005).

The University of Pittsburgh Medical Center (UPMC) strives to be a leader in the implementation of this technology. UPMC is the premier health system in western Pennsylvania and one of the most renowned academic medical centers in the United States. During the past decade, UPMC has reshaped the healthcare landscape in western Pennsylvania. With 19 hospitals and hundreds of other care sites, UPMC is unquestionably the predominant healthcare provider in the region. As the area's only academic medical center, UPMC is a hub for specialized services and innovative research programs and technology. UPMC utilizes cutting edge technologies, developed in-house and in partnership with commercial entities, to bridge the long distances between hospitals. Over the past few years, several UPMC hospitals have gone live with a full electronic health record, including full physician order entry. The electronic health record, referred to as eRecord, has been widely accepted and used by clinicians within many departments. Electronic Health Record technology is undeniably effective and efficient, however, in the event of a natural disaster or bioterrorism attack, this technology may be rendered ineffective and virtually useless due to a lack of electricity or internet connectivity.

Recent events, such as Hurricane Katrina, have shown the spotlight on the challenges associated with providing emergency care during a crisis situation. These events have also indicated an increasing need to provide interoperability between healthcare providers as well as between healthcare payers and providers on a patient-by-patient basis. Each patient has his or her own unique clinical and financial healthcare needs. Often, multiple healthcare providers are rendering these services with no interoperability. The management of patients both from a clinical and financial perspective is daunting with duplication of services and data collection.

In addition, healthcare providers and payers are faced with increased regulatory constraints, privacy and security laws, decreased budgets, demand for better health information access, and higher consumer expectations, all while a common technology infrastructure has not been established. Healthcare providers also are being faced with the difficult task of verifying eligibility of all individuals, while maintaining the confidentiality of sensitive patient information.

Hence, the healthcare community currently includes diverse and disparate systems that are not easily integrated, creating a nomadic patient atmosphere. Up to this point, the healthcare community has tried to address these issues in its unique and diversified way, resulting in unmanageable administrative processes, high operational costs, and ineffective provider communications. Specifically, the process for uniquely identifying patients is a manual process with no common key between foreign systems. Also, numerous point-to-point interfaces exist within systems. Furthermore, in present systems, paperwork is sent with a patient, information is verbally communicated from patient to provider at each visit. No common interfaces exist to

create inter-operability between different systems. During crisis situations, information is often unavailable and sometimes lost or destroyed.

Overview

The objective of this proposal is to meet the emerging need for a secure and portable means to carry patient-related information confidentially and to positively identify both the caregiver and the recipient of the care as well as facilitate management of emergency services during crisis. It is our recommendation that an integrated Healthcare Passport for patients, utilizing Smartcard technology (UPMC patent pending), be developed. The proposal will also include a secure access card that provides access to secure information and will carry credentialing information.

This card will be integrated into an Enterprise Provider Contact Database (EPCD) to facilitate communication between healthcare providers. The EPCD is a database of provider contact information. This information is continuously validated and tested through its daily use.

This card will be used by healthcare providers at all capacities. Additionally, UPMC has developed an application which, when used with the Smartcard, facilitates secure sharing of information and documents on various media between entities, in a one-to-one or one-to-many fashion (UPMC patent pending). This would facilitate secure transmission of encrypted data between locations. Using this technology, files stored in repositories could be encrypted to be readable only by specific authorized cardholders or groups. Unauthorized access to these archived files would yield only unintelligible data.

On a broader level, this recommendation will establish a platform aimed at addressing secure portable means to carry person-identifying information as well as critical clinical and financial information related to the patient during both non-crisis and crisis situations. This platform will be of value to the integration of government services, pharmacies, insurance providers, healthcare providers, emergency medical services, and clinics as well as healthcare facilities. It will provide the means to integrate ancillary services for patient-related services beyond the initial implementation and will be extensible to address future needs.

This information will not only be stored on a portable card, but on a regional data repository (RDR) which will be replicated at multiple regional sites which will aid in emergency situations as well at the recovery of information. The patient card will contain a snapshot of the Essential Patient Dataset (EPD), and will facilitate access to portable essential patient information when no network services are available. It will also facilitate authentication processes that positively identify the patient. To assure the currency and correctness of data stored on the card, patient data would be updated upon a visit to a healthcare provider during the course of everyday life.

These authentication processes may also be utilized on the provider side. The Smartcard supports computer authentication (access including automatic password management to disparate systems) and credentialing – SISAC. This functionality would be integrated with the Provider Contact Repository (PCR) and would allow providers to access patient information during routine services or emergency situation via the RDR. This card will also carry the provider's

credentials to be used as confirmation of credentials when no network services are available during crisis situation.

Applications to read the information can be available on stand-alone computers or laptops to facilitate downtime access or via the internet when network capability is available and an option. All information will be time and date stamped, as well as having the source provider of the information content. Each access to repository information will generate a log entry containing the identity of the authenticated user and a timestamp.

Figure 1: Smart Card Reader

Furthermore, a process has been developed utilizing Smartcard technology to securely share information on any computer media (including the internet) with multiple access functionality utilizing encryption methods – this product utilizes the SISAC product.

Technical Objective

The technical purpose of this initiative is to incorporate technology to assist individuals in communicating and transferring personal health information between various healthcare facilities and clinicians during both crisis mode and non-crisis mode.

At present the acceptance, usage and value of such tools and technology as an integrated system with Admitting Discharge Transfer (ADT) systems, acute care facilities and private practices are non-existent.

This initiative will facilitate processes in healthcare that directly impact the patient and multiple clinicians. Areas of improvement will include: 1) better knowledge transfer among patient to clinician and healthcare facilities; 2) improved decision making by clinicians based on personal health information regarding past medical treatment, tests results and current health status; 3) improved communication among patient, first responders and emergency department; 4) empowering and engaging the patient in the accuracy of their medical record; 5) improved efficiency regarding registration process to primary care practitioner (PCP) offices or acute care settings; and 6) portability of essential patient information that is accessible during a crisis situation.

There are several significant contributions that could be made as a result of this initiative. They include: 1) concise documentation and communication of current medications, known allergies, immunizations, past medical experiences, emergency contact information, and current chronic conditions between consumers and clinicians; 2) basic security services such as identification, authentication, integrity and accountability of usage by the individual; 3) protection of one's confidentiality regarding personal health data; 4) a means to empower and engage the patient in the content and accuracy of their medical record; and 5) portability of person specific information.

What is New or Novel about the Solution?

This solution is particularly innovative in its use of Smartcard technology to address both secure portable patient information and non-repudiated access and credentialing. This solution provides the security and portability of confidential patient information as well as a means to uniquely and positively identify patients leading the way to integration to disparate systems. This solution provides for secure access to patient information to a regional repository of information, with replication of information to provide backup capability in the event of a disaster and relocation of people. The government as well as healthcare providers will benefit by increased efficiency. Healthcare providers will have essential patient information available, in the event that critical medical information is lost or temporarily unavailable in crisis situation. The RDR can be used during crisis to proactively assess needs based on the statistics gathered from the data regarding age, conditions, allergies and immunizations, and match these with the services available.

Potential Benefits and Impact

The potential benefits and impact of such a system are difficult to quantify, however, we predict that they would be significant and wide ranging. In addition to allowing easy access to personal health information during a crisis situation, the Smartcard will have an impact and beneficial effect in all of the following areas:

- Patient Safety
- Information Security
- Fraud Prevention
- Cost
- Paperwork Reduction

University of Pittsburgh Medical Center Domain Expertise

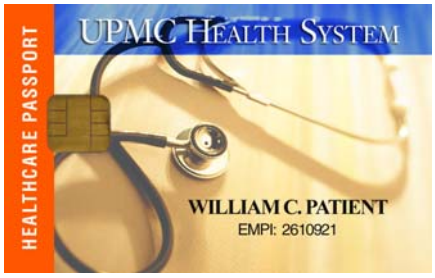

Figure 2: UPMC Smart Card

UPMC Information Services Department has developed a Smartcard – a credit card size device containing secure computer hardware – to electronically maintain patient data. This Smartcard has been utilized to deliver a Patient Healthcare Passport (Healthcare Passport) as a means to provide a secure means of transporting patient information confidentially. Integration of this functionality was primarily utilized within a physician office as a means of maintaining personal health information. Two additional products have been developed based on this Smartcard, that have not yet been implemented: 1) the secure credentialing card and 2) an implementation of this card to provide secure sharing of any information on any media.

An initial pilot implementation of a Healthcare Passport utilizing the Smartcard microprocessor card occurred in September 2001 with an issuance of 500 cards to UPMC Health Plan members that were patients at the Solano Practice in the Oakland office in Pittsburgh, Pennsylvania. The pilot initiative expanded to include 2,500 patients at the same practice with the most frequent visit history in September 2003.

Interfaces to the card have been built to expedite the registration process within a healthcare setting. With this implementation the process would be further extended to develop a self-registration process for patients at a kiosk (see Figure 3 for example kiosk screens). A website was developed to accommodate patients viewing their specific information online, and can be extended to updating emergency contact information.

Information currently on the card includes 1) Name/Demographics; 2) Medical record numbers from all clinical systems with site identification; 3) Insurance History obtained from registration systems; 4) Health Plan obtained from health insurance providers; and 5) Essential Clinical information obtained from clinical systems– drug regiment, allergies, immunization and problem list.

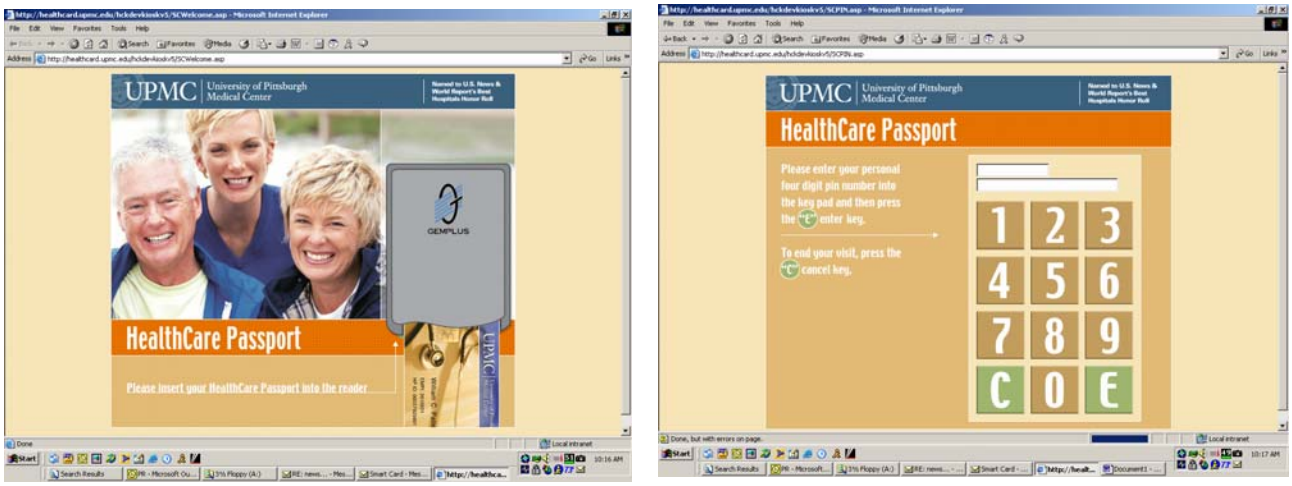

Figure 3: UPMC Smart Card Kiosk Screens

UPMC Responses to Questions Posed in the RFI

1. Approach, Finance, Sustainability, and Roles

a. What models and options are currently available that provide or support the capability to provide ready access to critical documents during or following an emergency?

(Overview page 4-6) UPMC has developed Healthcare Passport, a Smartcard project, which is being used within UPMC facilities currently and successfully. This usage tests and validates the program. The system allows access via Computer, PDA, or Laptop to patient information in an emergency or during routine healthcare services. The program consists of:

1. Patient Card: the card can be used for patient registration processing or at a remote kiosk (an access terminal similar to airline ticket stations) by the individual. Each use of the card provides an automatic update of essential patient information, with time and date stamp validation with every use. Patient information is also maintained in the Regional Clinical Data Repository. Access will be logged in accordance with HIPAA guidelines.
2. Provider Card: the card can access patient information from either the Patient Card or through the Regional Clinical Data Repository. The Provider Card also has provider credentialing information.
3. Information can be made available for emergency service through internet web access.

b. What models and options should be available, that are currently not available, to provide this service? Describe how this approach or model would work and illustrate with examples where useful.

(Overview page 4-6) Currently, this Smartcard model is available only through the UPMC system. UPMC plans to expand this system for use throughout Western Pennsylvania. The system could easily be adapted as a Regional Clinical Data Repository where essential medical information can be cryptically maintained and accessed through regional servers by computer, PDA or internet web access.

In emergency or disaster situations the patient would provide the card or the provider would access a Regional Clinical Data Repository for the essential medical information. In emergent situations, such as Hurricane Katrina, patient information would be accessible via internet web access, satellite transmission via Regional Clinical Data Repository with the use of a portable or laptop computer.

c. How will such a service be made accessible to those it is intended to help?

Individuals would have access to their personal information through the use of the Healthcare passport (either via a website or via their personal computer) or when receiving healthcare services via a kiosk. Emergency information would be accessible

through several sources: websites with secure capabilities such as Ready.gov, FEMA (and state emergency management websites), American Red Cross, and others. These providers would obtain the information from a Regional Clinical Data Repository. The Regional Clinical Data Repository will provide the critical essential information necessary for the management of required emergency services to the population in need.

d. How would accessibility for persons with special needs (e.g., persons with disabilities, persons who are not proficient in English) be ensured?

Displays can be selected by language of choice; headsets can be integrated for the blind at registration or kiosk locations.

e. What ownership, management, governance, financing, and sustainability issues arise as a result of the recommended approach, and how should these issues be resolved?

To expand the system for nationwide use, the card could be integrated into service by Healthcare Insurance Systems. However, to be a universally accepted system, Medicare and Medicaid would need to mandate this program.

f. How should the effort(s) be funded? Who should pay for the service and infrastructure?

The initial efforts should be initially funded via Medicare and Medicaid, by issuing the cards to those patients. The initial implementation of Smartcards as a replacement for Medicare/Medicaid cards could also be expanded to other health insurance carriers and healthcare providers as a universal health information system. Universal use of the Healthcare Passport would provide positive personal identification reducing the potential of healthcare fraud and identity theft. Regional Clinical Data Repository servers and internet access for emergency operations would save its own cost for emergency/disaster response under the National Response Plan by providing required critical information for responders via the National Incident Management System.

2. Function, Capabilities, and Performance

a. What types of information do you view as relevant, necessary, or useful to access in an emergency (e.g., birth certificates, wills, medical information)? Of these types of information, which would be easy to deposit with the type of service contemplated in this Request for Information (RFI), which would be difficult, and why?

> For emergency medical response, the system will need to maintain Personal Identification including a digital photograph and essential medical information (EMI) such as: blood type, allergies, vaccinations, medications, and personal medical conditions (i.e., diabetes or coronary condition, etc). Provider Cards will require the maintenance of information that will validate the provider's credentials in emergency/disaster situations.
>
> The amount of information available could be, essentially, unlimited. To ensure the trust and acceptance of the citizenry, however, requiring more than the most basic personal identification and EMI will likely hinder public acceptance.

b. What is the best approach for storage and retrieval of this information?

> The primary storage application will be via the portable Smartcard that will remain in the possession of the individual patient and provider. This process provides accessibility under less than optimal conditions. In situations such as emergencies or disasters when the Smartcard is lost or unavailable, the information would be replicated in and available for download from Regional Clinical Data Repositories. This information would then be accessible through a secure internet web portal to providers.

c. What limits should there be on the availability of information via the service contemplated by this RFI, and how should those limits be implemented?

> HIPAA guidelines should be adhered to in implementation. The Smartcard provides positive, non-repudiated identification of the provider and the patient. Access to information could be tiered with personal identification information immediately available much like a driver's license. Access to other information such as medical records could be accessed securely by a credentialed provider.

d. What are the necessary features, capabilities, and attributes of the service contemplated by this RFI?

- A portable token (Smartcard) with cryptographic and storage capabilities which facilitates the identification and storage of critical EMI.
- A portable application which may be used on a PC or PDA to obtain emergency information from the smart card. This would be used where there is no network connectivity, or (with appropriate secondary authentication) in the event the cardholder is unable to present a PIN to the card.
- A web based application to authenticate the individual, route requests to the appropriate repository, and provide a secure path for data back to the individual.

- Secure – Sensitive information contained on the Smartcard is protected by hardware barriers which detect and prevent physical tampering attempts. The card operating system also implements security routines which handle authentication for file and crypto access and encrypt card communications.
- Trusted – The Smartcard is personalized with a user - unique keyset and secured by an approved vendor prior to distribution. The successful completion of a Smartcard authentication transaction and establishment of a secure communication channel between a web client and application server provides a trusted relationship between both parties.

e. How should this service support disaster survivors in providing documentation necessary to obtain federal, local, and non-governmental disaster relief benefits?

In a disaster situation, this system will identify the individual and provide critical information needed for immediate medical care. Additionally it can be used to access data required for disaster relief. Information required for forms and documents for relief benefits will be readily available on the card or accessible online. Use of portable kiosks at a disaster site would allow individuals access to their information, as well as recover their information online.

f. What are the performance requirements of the service or the system that supports it?

The system will allow for real-time access to information. It will be available for use 24/7, with replication to a Regional Clinical Data Repository. The Smartcard system would be a daily-use tool, updating the information upon receipt of healthcare services or individual input ensuring accuracy and currency of the information. Regional Clinical Data Repository servers will provide full redundancy.

g. What disclosures should be required and under what circumstances or conditions would such disclosures be made?

As part of the enrollment process, users would be required to sign a user agreement. The user agreement should clearly describe the uses of the information contained within the system and what privacy the individual can expect. If a user declined to sign the user agreement, their information could not be stored within the system. Sample terms of user are provided in Attachment E.

3. Rights, Rules, Responsibilities, and Enforcement

a. Whom do you view as the interested parties? How should interested parties interact? What are their roles and responsibilities?

Potential interested parties include: healthcare providers, patients, government offices and government services. Information would be available to these parties on an as needed basis. Currency of the information would be the critical responsibility for both provider and patient. The currency of information would be automatic with daily use of the card or by online entry to the Regional Clinical Data Repository by the provider. All participants would be responsible for feeds to the repository, with the appropriate data. The patient and providers would be responsible for confirming the accuracy of the information. All information would be time and date stamped with credential information from the party that supplied the information. When discrepancies arise, only the party that supplies the information would be able to change or correct the information. The patient can make notes to any information that they do not provide.

b. What is an inappropriate disclosure? Who has liability for inappropriate or unlawful disclosures, or harms that come as a result of storage of personal data?

An inappropriate disclosure of information would be as defined in the user agreement. If HIPAA was deemed to apply to the system, inappropriate disclosure of information would consist of the release of personal and private information without the express written consent of the individual, except as defined in 45 CFR 160-164.

Liability for the disclosure of such information shall fall on the custodian of the information.

c. What enforcement mechanisms are appropriate to protect information, and who should be responsible for enforcement?

Access to information through the Smartcard would be coded and require 'log-in' by the patient or by a provider with a coded card. Information availability online will also be coded for access. All information would be protected in accordance with the user agreement and relevant state and federal regulations. The provider of the services must bear the direct responsibility for enforcing and ensuring that the appropriate protections are in place to protect personal and private information.

d. What rights should individuals who deposit their information have with respect to the custodian?

Individuals would have the right to access and retrieve their personal health information at any time via the web portal or via a kiosk. Individuals would also have the right to have their information removed from the system. These individuals would also have the right to assume that the custodian will safeguard the information consistent with applicable federal and state laws.

e. What rights should be assigned to custodians providing the service?

Custodians of the information will have the right to access information only to the extent at which is needed to manage the information and make it available consistent with the consent documents or federal or state laws.

f. What data disclosure laws and policies should apply? Who will have access to the information, and under what circumstances?

Data disclosure requirements will be primarily governed by the user agreement.

Only the individual, the provider, health insurance providers, Medicare and Medicaid, and the federal administrative agency charged with the management of the Smartcard system will have access to the information. Access to the information will be provided on an as-needed basis. The individual will have complete, unrestricted access to their own information. All others will have access, on an as needed basis, to EMI and basic patient identifying information. Other information contained on the card will require the patient's consent to access. For example, in the event of an emergency, where the patient is unconscious, the healthcare provider could access the patient's EMI, utilizing a card reader and their own provider card, but no other information stored on the card would be accessible to the provider. Custodians of the information will have the right to access information only to the extent which is needed to manage the information and make it available consistent with the consent documents or federal or state laws.

g. What other types of rules should apply to the service?

The primary rules and regulations guiding this service are state and federal information privacy and security regulations such as HIPAA.

h. What legal implications are there, if any, of storing electronic copies of important documents and making them available via such a service to those permitted to receive the information? If there are impediments, how should they be overcome? (For example, how will the contents of documents be authenticated?)

i. If residents of one State are permitted to store their documents in another State, how would protections travel across States?

This system is predicated on a patient enrollment process that clearly describes the uses of the information and what privacy the individual can expect. These protections would travel with the information across State lines. In addition, the information housed on the Smartcard and in the Regional Data Repositories would be protected under federal law.

4. Security and Standards

a. What administrative, technical, and physical security approaches should be considered?

- Encryption of data and communication channels, PIN/Password Protected Cards.
- Freedom of Information Act, 5 U.S.C. 552, and Part 5 of this title.

b. What security standards mechanisms, if any, should be adopted by or imposed on the custodians?

In addition to maintaining industry standard security measures (such as digital encryption), at a minimum, HIPAA security standards should be imposed on the custodians.

c. How will access and authentication controls be implemented?

Authentication begins with the user entering a PIN when the Smartcard is inserted into a card reader. PIN lengths and retry limits for this operation are configurable. If an incorrect PIN is entered more times than is allowed by the retry limit, the card locks itself preventing further access attempts. The Smartcard contains keys unique to each individual which provide a 1:1 match during authentication. Keys present on the Smartcard may also be used to establish a secure connection to the remote application.

The entire Smartcard authentication process would be completed in a matter of seconds and could be as follows:

1.	Component helper application on client launches login
2.	User enters PIN (password written to card on 1st time login)
3.	ActiveX component on client presents PIN to card
4.	Card responds with user ID and password
5.	Values input
6.	Authorization takes place
7.	Server generates random challenge and passes to card via client component
8.	Card encrypts challenge and passes back to server
9.	Server verifies variable accordingly and sets or clears session
10.	Outside requests will be checked and required to have a Smartcard
11.	Application checks user group for username and allows or denies access to patient information
12.	Application presents patient information based on previously established relationships

d. What technical, data, format, or performance standards should be considered?

Encryption, XML format of standardized data, real-time access for updates and direct feeds to Regional Clinical Data Repository servers as patient is seen by provider.

e. How will the identity of the individual requesting information be verified?

Each smart card will contain a unique asymmetric key set for authentication. One of the keys remains securely on the card and is never disclosed, the other is public. When the user presents the correct PIN to the Smartcard, within the allowed retry limit, the internal key is enabled for use. A challenge is made to the card by the remote service based on data encrypted with the public key. The card processes this challenge with its private key and returns the result to the remote service. This data should match the original unencrypted challenge.

5. Potential Federal Roles

a. What role, if any, should the federal government play in encouraging the development of services whereby individuals can voluntarily deposit their personal identifying information for access during or following an emergency?

Applying this system as a requirement for Medicare and Medicaid would insure application throughout the national healthcare system. The deposit of information must remain within the limits of minimal required essential medical information and personal identification information will be acceptable by the majority of the public. Additionally individuals will retain possession of their card and have access to their information encrypted and secured by use of a PIN.

This system could easily be adopted as a standard and fulfill the HIPAA requirement for a National Identification Card.

b. What role, if any, should the federal government play in encouraging citizens to voluntarily collect and store their personal information for access during or following an emergency?

If the system is applied to Medicare and Medicaid, the federal government could then encourage insurance health plans to adopt the system. Healthcare providers would have to use the system for Medicare and Medicaid patients and could be encouraged to recommend the system to all of their patients allowing them to use the system as a record of services provided. The system will allow a method to uniquely identify patients across disparate healthcare systems across the nation.

The federal government could easily implement this system as a National Identification Card.

Appendices

Appendix A: Illustrative Diagram

The following diagram illustrates the relationship of the Smartcard solution to Emergency preparedness, response, and recovery.

Appendix B: Vision – The Individual Experience

Individuals will receive a Healthcare Passport to track and maintain their personal health information and EMI. This Healthcare Passport will utilize the secure portable Smartcard technology. This card will permit the patient to access selective information from their own medical record information from home (provided they have a Smartcard reader) or from strategically located kiosk workstations throughout the health system.

This card will be personalized with the individual's personal information to ensure that the individual can move seamlessly and efficiently between healthcare providers (i.e., personal physicians, hospitals, specialists). The card will provide the means to streamline the registration and reimbursement process as well as improving the accuracy of the data collection process and removing the current duplication of data collection. General medical and insurance information will be securely held internally on the card in an encrypted format. Secondary insurance information and limits, rules for use and reimbursement, effective dates, and co-pays can be included on the card. Any unauthorized use of the card will deactivate the card until the card is reauthorized. Missing and lost cards will be deactivated as well. This can be done offline (without the card being available).

Medical alerts, conditions, allergies, blood type, drug regimen, vaccinations, general medical background, and demographics will be readily available on the card. With the appropriate security, information can be accessed from the card during routine care as well as in emergency situations.

The patient will be able to remotely access secure features related to their patient care to update changing information, notify their physician when necessary, schedule appointments as well as receive electronic notification of their upcoming appointment. Cards can be updated remotely at all/any locations equipped with a reader. The card will be time and date stamped to track the current state of the information.

Home monitoring equipment may be modified to accept the card to record patient vital statistics on the card to be used by the caregiver. This information can be uploaded from home or the card brought in at the next visit for accurate collection of information. Although the uses are unlimited, situations where this is being considered for use are: heart monitors, blood pressure reading, CPAP machines (sleep study devices), SIDS(sudden infant death syndrome) equipment, and sugar levels for diabetes.

To further improve the patient experience, the card could be enabled with cash value to be used as co-payments for care, at the gift shop or cafeteria, and for facility access. Relationships with banking institutions could be pursued to assist in payment methods for these services.

Appendix C: Biographical Information

UPMC has significant experience in the development of novel Information Technology Solutions, as well as Bioterrorism Preparedness, and overall provision of quality healthcare. Biographical sketches of the following individuals provide evidence of this expertise:

- Brian Adams
- Charles Boivin
- Kathleen Criss
- Scott Gilstrap
- Christine Henderson
- Robert Schwartz
- Loren Roth

Brian Adams is an expert in information technology and digital encryption. As part of his extensive background in information technology he has served in the following capacities:

- Developer for Smartcard Initiative – from Health Plan Perspective in Sept 2001 – with 500 cards issued
- Developer for Smartcard Initiative – from Health System Perspective in Sept 2001 – with 2,500 cards issued
- Developed FAT, VOP 2.1 based operating system for AT90SC6464C based Smartcard
- Developed applications for interfaces to inpatient and outpatient registration systems
- Developed client and server side applications for Smartcard interface and mutual authentication
- Developed security applications for Windows logon utilizing Smartcard
- Developed compression and data integrity systems for the Smartcard
- CEO of hardware and software consulting business – Designer Circuits
- Analog / Digital / RF circuit developer and designer
- Microcontroller based design and programming in C and Assembly for Atmel, Signetics, Motorola, Intel, AMD, SGS Thompson, TI, Microchip, Zilog product lines
- Win32 Device driver development
- Microcontroller-based black box interface development
- Developed advanced security methods when utilizing the Smartcard or internally encoding data within Smartcard

Charles Boivin II is the Disaster Management Research Coordinator for the University of Pittsburgh Medical Center, Pittsburgh, PA. Chuck is assigned to the Innovative Medical and Information Technologies Center and responsible to assist in the development of a Disaster Management Center for UPMC and to coordinate disaster response activities within the community and region. He also is a major contributor for the community coordination for the new Regional Joint Readiness Center to be located at the 911 Airlift Wing, located at the Pittsburgh International Airport, PA.

Kathleen Criss, CBCP is the Director of the UPMC Disaster Management Center. Ms. Criss is an expert in the area of disaster and emergency management. In addition to her extensive professional experience in this area, Ms. Criss also serves on the Department of Homeland Security/Department of Health and Human Services, Healthcare Sector Coordinating Council, the ASME Innovative Technologies Institute, LLC, RAMCAP™ Consensus Standards Committee, the Business Continuity Planning Workgroup for Healthcare Organizations (BCPWHO), the Pittsburgh Regional Business Coalition for Homeland Security, Operations Council, the PA Statewide Advisory Committee, Strategic Medical Assistance Resource Team and the Southwestern PA Emergency Response Group (PA Region 13), Healthcare Subcommittee.

Scott Gilstrap is the Vice President, IMITS Center at UPMC. From 1988 until 1991, Mr. Gilstrap served as an Aeromedical Evacuation Technician, 13 AFMC, US Air Force, Clark AB, Philippines. From 1991until 1997, Mr. Gilstrap served as a NCOIC, Medical Information Systems, 86 AES, US Air Force, Ramstein AB, Germany. Since that time Mr. Gilstrap has worked in Information Technology, developing and implementing information technology solutions.

Christine Henderson has an extensive background in information technology. She has participated in and led projects to develop innovative solutions to complex problems. Her experience includes:

- Leading the implementation and deployment of Smartcard /Healthcare Passport from Health Plan perspective in September 2001 with 500 cards issued
- Leading the implementation and deployment of Smartcard /Healthcare Passport from Health System perspective in September 2002 with 2,500 cards issued
- Developing COM based interfaces to inpatient and outpatient registration systems
- Developing applications for kiosk
- Developing web applications for Smartcard updating, viewing and printing.
- Developing active directory based security systems for web applications.

Loren Roth, MD, **MPH**, is the Senior Vice President, Quality Care and Chief Medical Officer at the University of Pittsburgh Medical Center (UPMC); Associate Senior Vice Chancellor for Health Sciences, University of Pittsburgh; Professor of Psychiatry, University of Pittsburgh School of Medicine; and Professor of Health Policy and Management, University of Pittsburgh Graduate School of Public Health.

Dr. Roth is former Chairman of the University of Pittsburgh's Health Sciences-Wide Panel on Medical Ethics.

In his role as Senior Vice President, Quality Care and Chief Medical Officer of UPMC, Dr. Roth directs quality improvement activities across the healthcare system, provides overall supervision for residency training and works with University faculty and administrators, community hospitals/physicians and insurers to link the Academic Medical Center with the Southwestern

Pennsylvania healthcare community and assure UPMC's success in the cost-effective healthcare environment.

Since September 2001, Dr. Roth has led the UPMC's planning efforts for preparedness in the event of a terroristic event in this region. He received the Senior Vice Chancellor's Extraordinary Service Award in recognition of his efforts in conceptualizing and coordinating the implementation of a biodefense infrastructure for the University of Pittsburgh, UPMC, and the western Pennsylvania community.

Dr. Roth has made seminal contributions to planning and execution of the student curriculum of the University of Pittsburgh School of Medicine. He was the Co-Coordinator for the University of Pittsburgh Medical School's curriculum for the Patient/Doctor Relationship Block and Co-Director of the "Introduction to Being a Physician" course for first year medical students. Dr. Roth has twice received the Outstanding Teacher Award from the WPIC psychiatric residents.

Robert Schwartz, MD, MPH, FACEM, FACPM is the Medical Director for Physician Relations at the UPMC Health System has the responsibility to conceptualize, organize and operationalize the Office of Physician Relations. The mission is to maximize the quality of services to independent practitioners to improve relationships, generate loyalty, increase referrals and impact the quality of care. These goals have been exceeded in the first year of the program. For example, acute inpatient referrals have been increased 27% over the last 2 years. There has been rapid expansion of the Physician Affiliation Program, increased membership by Independent Physicians, resulting in improved physician-to-physician communication, physician satisfaction with the Health System and patient referrals. Inpatient referrals from Affiliated Physicians were increased 14.8% from community-based physicians and 21% from Emergency Departments. Utilizing the principles of mass customization, the program was individualized to fit the specific needs of various physician groups.

Dr. Schwartz has been instrumental in successfully bridging the gap between operational management and contributions to strategic vision, new software was created, supported by re-engineering of the associated business processes for widespread, accurate and timely communication to approximately 10,000 physicians in Western Pennsylvania. These tools have become the cornerstone of the Terrorism Response & Information Center, which contributes to keeping physicians informed (Health System Alerts) and a personalized conduit for physicians to communicate with colleagues. This new communication process functions as a daily monitor for Health System operations and serves as the 'central nervous system' for communications and notifications. Physician satisfaction with the referral and communication process is greater than 92% approval ratings.

In addition to the responsibilities, Dr. Schwartz continues the clinical practice of Emergency Medicine in several community hospitals.

Appendix D: Related Website

For additional information regarding the UPMC Healthcare Passport solution please refer to the following websites:

- The UPMC Healthcare Passport Website (https://healthcarepassport.upmc.com)

Appendix E: Sample Terms of Use

The following Terms of Use are provided to users of the UPMC Healthcare Passport and are offered as an example of the type of terms of use that could be offered under the proposed response.

Terms of Use
University of Pittsburgh Medical Center (UPMC) is pleased to offer you the ability to view parts of your medical record online by using the UPMC Healthcare Passport.

The UPMC Healthcare Passport is based on Smartcard technology. Smartcards, though similar in design to a credit card, are capable of securely storing information. In this case, the Healthcare Passport will be used to store your insurance and medical information. Using the UPMC Healthcare Passport and UPMC Healthcare Passport website, the Smartcard can be used to access this information.

By applying for the UPMC Healthcare Passport you acknowledge that you are requesting access to your insurance and health information via the UPMC Healthcare Passport. UPMC grants you a non-transferable and limited right use the UPMC Healthcare Passport to access your medical information that is contained on the Smartcard.

Please read the following terms and conditions carefully before completing your registration for the UPMC Healthcare Passport. By requesting a UPMC Healthcare Passport and signing the UPMC Healthcare Passport Application form, you agree to be bound by the following terms and conditions every time you use the card. Failure to follow these terms and Conditions may result in your termination of your enrollment in the UPMC Healthcare Passport.

Eligibility:

Participants must be 18 years or older to be eligible to participate in the UPMC Healthcare Passport. Patients must be active patients of a UPMC physician who has elected to offer the UPMC Healthcare Passport to the physician's patients. You agree to contact UPMC within a reasonable period of time should you decide to no longer use UPMC to provide your medical care.

User ID and Password:

To receive a UPMC Healthcare Passport you must sign the UPMC Healthcare Passport Application form and submit it to your physician's office. Once your identification is verified a UPMC Healthcare Passport will be provided to you. Your UPMC Healthcare Passport will not be given to any other person. You will also be provided with an initial password which you will use to access your UPMC Healthcare Passport.

Should you loose your UPMC Healthcare Passport or forget your password, you should contact your physician's office. There will be a 48-hour turnaround time during regular business hours in response to your call.

Your Use of the UPMC Healthcare Passport:

By requesting to participate in the UPMC Healthcare Passport you understand and agree to the following:

- You confirm that all information supplied by you is true, complete and accurate in all respects and you agree to notify us within 30 days of any changes to that information.
- You shall only access the website as permitted by us and shall not attempt at any time to circumvent system security or access to any source software or compiled code.

Provision of services:

UPMC agrees to provide the UPMC Healthcare Passport to you free of charge to assist you in accessing your medical information.

While every effort is made by UPMC to make the UPMC Healthcare Passport free from error, UPMC cannot guarantee the accuracy, adequacy or completeness of the information contained on the UPMC Healthcare Passport. Additionally, UPMC cannot guarantee that the UPMC Healthcare Passport will fault-free, but will endeavor to correct reported faults as soon as we reasonably can.

UPMC may change the UPMC Healthcare Passport from time to time. Additionally, UPMC may suspend or terminate the whole or any part of the UPMC Healthcare Passport at any time. UPMC may also provide links to other website or resources from the UPMC Healthcare Passport but neither accepts responsibility for them nor endorses their content.

Surveys:

As a participant of the UPMC Healthcare Passport on occasion you may be asked to complete patient satisfaction surveys via the UPMC Healthcare Passport. UPMC may use that information to enhance the UPMC Healthcare Passport functionality or analyze the data as part of studies and reports. In these cases, all identifying information will be removed.

Privacy Policy:

UPMC is committed to complying with all federal, state, and local laws, as well as applicable regulations, standards, and guidelines established by governmental agencies and accepted accrediting organizations.

Additionally, UPMC's HIPAA Notice of Privacy Practices can be found at:

http://www.upmc.com/NoticeOfPrivacyPractice.htm

Security:

The UPMC Healthcare Passport is protected using industry standard security measures. While such security reasonably protects your information and use of the UPMC Healthcare Passport, if you have concerns regarding the security of your information or the use of the internet to communicate your personal or health information you should consider not enrolling in the UPMC Healthcare Passport.

To access the UPMC Healthcare Passport you will be issued a UPMC Healthcare Passport and password. You are responsible for the security and proper use of your the UPMC Healthcare Passport and must take all reasonable steps to ensure that it is kept confidential and not disclosed to any unauthorized person. If at any time you feel that the confidentiality of your the UPMC Healthcare Passport has been compromised, you should change your password.

You understand that UPMC takes no responsibility for and disclaim any and all liability or damages arising from others accessing your insurance or health information due to you sharing or losing your the UPMC Healthcare Passport or password and contact your physician's office.

If UPMC has reason to believe that there is likely to be a breach of security or misuse of the UPMC Healthcare Passport, your participation in the UPMC Healthcare Passport may be discontinued by UPMC without prior notice.

Disclaimer:

While UPMC will attempt to offer the UPMC Healthcare Passport without interruption, access is provided on an "as-is, as-available" basis. UPMC does not guarantee that you will be able to access the UPMC Healthcare Passport at any particular time. Additionally, UPMC cannot guarantee that the Website will be error free. Should you have reason to believe that your information on the UPMC Healthcare Passport is not accurate or that there is an error with the UPMC Healthcare Passport, you should contact your physician's office immediately. Additionally, UPMC reserves the right to terminate your access to the UPMC Healthcare Passport at any time without cause.

YOU UNDERSTAND THAT THE UPMC TAKES NO RESPONSIBILITY FOR AND DISCLAIM ANY AND ALL LIABILITY ARISING FROM ANY INACCURACIES OR DEFECTS IN THE INFORMATION, SOFTWARE, COMMUNICATION LINES, THE INTERNET OR MY INTERNET SERVICE PROVIDER (ISP), COMPUTER HARDWARE OR SOFTWARE, OR ANY OTHER SERVICE OR DEVICE THAT YOU USE TO ACCESS THE UPMC HEALTHCARE PASSPORT. ADDITIONALLY, YOU ARE RESPONSIBLE FOR PRINTING COPIES OF YOUR INFORMATION IF YOU WANT TO HAVE THE INFORMATION AVAILABLE IN THE EVENT THAT THE UPMC HEALTHCARE PASSPORT IS UNAVAILABLE.

E-Mail and UPMC Web Site Terms:

The UPMC Healthcare Passport and your use of the UPMC Healthcare Passport web site is additionally governed by UPMC's website terms (including privacy policies, disclaimers and e-mail and electronic communications terms of use), found at:

http://www.upmc.com/TermsOfUse.htm

Any electronic communications you have with UPMC are governed by the terms described in the section titled “E-MAIL TERMS OF USE”.

General:

We may modify these terms and conditions, the UPMC Healthcare Passport or the content of the associated website at any time. For this reason, you should review these terms and conditions on the UPMC website periodically.

The services and the content of My UPMC are protected by copyright, trademark and other intellectual property concepts, as applicable and are provided solely for your personal use. Republication, distribution or use of the UPMC Healthcare Passport that is inconsistent with the terms and conditions described herein is strictly prohibited.

These terms and conditions are governed by and will be interpreted in accordance with the laws of the Commonwealth of the Pennsylvania.